Triplet Authentication System for Efficient Quality of Service in Vehicular Ad hoc Network

By Muhammad Anwar Shahid (shahi116@uwindsor.ca)

Abstract –

Vehicular Ad hoc Network (VANET) is a type of network derived from Mobile Ad hoc Network (MANET). Authentication plays a major role in VANET for the providence of secured communication among vehicles [1]–[3]. Authentication in this network is achieved by cryptography techniques, signature algorithms and message verifications. In VANET, the vehicles share some sensitive information related to safety and hence the need for authentication is high. Authentication schemes in VANET are studied in several research papers in recent years. In [4], authentication was provided for performing secure data transmission based on the identity. Identity was the major parameter considered with which the data was encrypted and forwarded to other vehicle. Hereby the data was decrypted and retrieved first and then Identity was verified. A lightweight authentication was proposed for performing three different mutual authentications [5]. The vehicles those are moving at similar velocity were defined into a cluster in which a head node was chosen based on trust values. Clustering based on this metric involves more number of vehicles into a cluster or only few vehicles in a cluster. Both the processes of clustering and head selection need to be repeated. Similar procedure is followed for all the three authentication which is concluded with a password update phase.

Authentication was also provided by using certificates which is uniquely generated for each vehicle. An efficient privacy preserving authentication and key distribution technique was proposed for distributing group keys [6]. The vehicle registers into trusted authority with identity and other credentials, these are required during authentication. Trusted authority generates fake identity for each vehicle to provide security. This entire authentication failed to minimize the working of trusted authority. Identity Based Online / Offline Signature scheme was proposed in [7]. This scheme follows setup, extraction, signature generation (Online using online key, Offline
using offline key) and verification. The keys involved in signature generation are varied periodically which leads to complexity and the use of RSA algorithm consume higher time.

An anonymous authentication protocol was presented based on cooperative authentication method [8]. Using this protocol group keys are periodically generated and distributed by trusted authority. The keys are managed by the construction of a tree that consumed higher storage due to the increase in keys. Another scheme called conditional privacy-preserving and authentication was proposed to optimize signature generation and verification [9]. This scheme used pseudonym based signature for identity authentication. More than one hash value and pseudonym identity is involved which makes this scheme complex. Dynamic Pseudonym was proposed based on traffic aware VANET environment [10]. Traffic-Aware Pseudonym Changing Strategy was presented in which traffic density is noted and pseudonyms are changed. But the traffic density in VANET is not the right choice for changing pseudonym. Dual authentication and key distribution technique was presented to enhance quality of Service [11]. Two special parameters are computed by trusted authority for generating signature. Authentication is performed only by the trusted authority using this technique. One-time identity based aggregate signature technique was proposed in which multiple trusted authorities are involved in the environment [12]. However several authentication schemes were proposed, they exist with some limitation which needs to be resolved. Previous works aimed to provide security either for Vehicle to Vehicle Communication or Vehicle to Infrastructure Communication.

To overwhelm the authentication problems existed in VANET, we have proposed a novel VANET architecture. Many previous research works have focused authentication only for single type of communication. Our aim is to concentrate authentication in entire VANET wherever the communication is held. The proposed VANET is comprised of Vehicles, Roadside Units (RSU), Trusted Authority (TA) and Authentication Server (AS). Authentication is provided between the following entities (1) Vehicle to Vehicle authentication, (2) Head Vehicle to RSU authentication and (3) RSU authentication. Each authentication is performed by an entity which is in higher position than itself. For faster authentication the vehicles are grouped by using **Four-Quadrant Partitioning**. The road lane is equally divided into segments of equal area, for instance say 100m. In each segment mid-point is predicted and the segment is partitioned into four parts, in which the vehicles in two parts move in same direction and the other two parts in opposite
direction. Head vehicle in each part is chosen based on these metrics trust value, node degree and mobility speed using **Firefly algorithm**.

Each vehicle and RSU is registered to TA and the information is shared with AS for the purpose of authentication. Vehicle registers with a unique fingerprint and Identity, whereas RSU registers with unique identity and password. The RSU’s password is static and it cannot be changed. The process of each authentication is illustrated below:

(1) **Vehicle to Vehicle Authentication**:

Vehicle to Vehicle communication is involved in VANET for sharing information between vehicles. This authentication is performed using Time based Diffie Hellman algorithm in which time is included for faster authentication. The parameters taken in account for this authentication are fingerprint and token. The fingerprint is converted into binary and while authentication XOR operation is performed for verification. Token is a unique entity that consists of vehicle ID and its signature. Signature is generated using ECDSA and all the parameters are verified by other vehicle.

(2) **Head Vehicle Authentication**:

Each head vehicle is authenticated by RSU present in its communication range. RSU authenticates the head vehicle by verifying location, a unique point which is provided by TA during the election of head and Quadrant ID. These values are encrypted using Homomorphic encryption along with a timestamp and forwarded to RSU for verification. After authentication the head vehicle access data, if failed it is reported to TA.

(3) **RSU Authentication**:

RSU is authenticated by TA periodically to ensure that RSU is legitimate in the network. RSU ID and Password is verified for authenticating an RSU, here encryption is not used since the channel between them is secure.

Our proposed VANET is executed and their result achieves better performances in terms of the following Quality of Service metrics as:

1. Throughput
2. Delay with respect to number of vehicles / time
3. Packet Delivery ratio with respect to number of vehicles / time
Proposed VANET Architecture

**RSU Authentication**
- RSU ID
- Password

**Head Selection (Firefly Algorithm)**
- Trust value
- Node degree
- Speed

**Head Authentication (Quadrant ID, Location & Point)**
- Homomorphic algorithm

**V2V Authentication (Fingerprint & Token)**
- Time based Diffie Hellman
- ECDSA

**Vehicles moving direction**

**Segments**
- S1, S2

**Quadrants in S1**
- P11, P12, P13, P14

**Four Quadrant Partitioning**

**AS**

**Head Vehicle**

**Request for Vehicle’s signature and fingerprint**

**Head Authentication**
- Quadrant ID, Location & Point
- Homomorphic algorithm

**TA**

**RSU**
Reference Explanation

REFERENCE 1

TITLE – A Survey on Authentication Schemes in VANETs for Secured Communication

Concept –

This paper discusses all about the secured and authentication schemes that are involved in VANET. The major attack types are studied due to which the need of secured communication is required. Requirements of security in VANET are entity authentication, message authentication, privacy, no-repudiation, traceability, communication overhead and computation overhead.

REFERENCE 2

TITLE – VANET Security: Issues, challenges and solutions

Concept –

This paper elaborates the need of security in the highly dynamic connections to share sensitive information. The designed security mechanism in VANET also needs to cope up with the common challenges as mobility, error tolerance, latency control and key management. Also different attacks are classified based on the membership, activity and intensions.

REFERENCE 3

TITLE – A review on VANET security attacks and their countermeasure

Concept –

Security issues existing in VANET are discussed in this paper and also MANET and VANET are compared with respect to different parameters. Different attacks and the techniques used for prevention are listed out with respect to the limitations existing in those technologies.
REFERENCE 4

TITLE — Efficient identity-based data transmission for VANET

Concept —

In this paper, the authors have proposed an identity based data transmission protocol that makes use of Lagrange interpolation to achieve integrity. The Trusted Authority participating in this environment is responsible for generating private keys for itself, RSU and vehicle. The data are encrypted before transmitting to a receiver; the encrypted cannot be retrieved without the private key.

Problems —

- An entity is verified only after decrypting the original message, this is improper since the verification must be performed before retrieving the original message.
- Each entity’s identity is only taken into account for key generation

Solution —

- On completion of authentication the data is received
- More than one parameter is considered for each authentication

REFERENCE 5

TITLE — Design of Lightweight Authentication and Key Agreement Protocol for Vehicular Ad Hoc Networks

Concept —

This paper proposes three different authentications between (1) vehicle to vehicle, (2) vehicle to cluster head vehicle and (3) cluster head vehicle to roadside unit. The vehicle with higher trust values and stronger connectivity is chosen as cluster head. Vehicle to vehicle authentication is initiated from the generation of random nonce, if vehicle authenticates then single session is shared for communication. This similar authentication procedure is followed for other two types
proposed in this paper. Vehicle registered in trusted authority can changes its password using its unique identity and prior password.

**Problems** –

- Each vehicle registers with its unique identity and password in trusted authority, but as per this work the user is enabled to change password without the knowledge of trusted authority. The changed password is not updated in trusted authority.
- Repeated clustering and head selection

**Solution** –

- Vehicles are grouped with respect to the partition of road lane and hence partition can be performed only once.
- Vehicle registers with unique Identity and fingerprint

**REFERENCE 6**

**TITLE** — Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks

**Concept** –

An anonymous authentication approach is proposed in this paper for achieving data integrity. This approach includes privacy preserving anonymous authentication scheme and privacy preserving anonymous key distribution. During authentication trusted authority generates a fake identity for each vehicle without the knowledge of vehicle for privacy.

**Problems** –

- In authentication scheme a shorter lifetime certificate is generated, hence this scheme requires repeated computation of certificate.
- Here the receiver would be trusted authority which needs to perform more computations, this result with more burdens over trusted authority.
Solution –

- Each entity has its own responsibility and hence burden at trusted authority is reduced

REFERENCE 7

TITLE – Secure Vehicular Communication Using ID Based Signature Scheme

Concept –

In this paper the authors have proposed ID Based Signature (IBS) and ID-Based Online / Offline Signature (IBOOS). In IBOOS scheme, offline key is used for generating offline signature and online key is used of online signature. Both the keys are periodically changed that means the signatures also changes. In this work, for transmitting emergency messages RSA algorithm is used. Pseudo identity is involved for authentication, which is generated by the vehicle itself. Pseudo ID is generated from the broadcasted public key of RTA and then authenticated.

Problems –

- RSA algorithm consumes higher time for key generation and decryption.
- Pseudo ID is also applicable to be generated by malicious vehicle, since RTA’s public key is broadcasted and it does not authenticate receives

Solution –

- Security related parameters are sent only for the requested vehicle i.e. it is not broadcasted.

REFERENCE 8

TITLE – Reliable Cooperation Authentication for Vehicular Networks

Concept –
A cooperative Authentication method is used in this paper which proposed an Anonymous authentication protocol. In this proposed work two-layer pseudo-identities generation method is involved. Pseudo identities are generated for time window and for time slot. The generated keys are updated by roadside unit based on the construction of b-tree.

**Problems** –

- Too many mathematical computations.
- The length of the tree increases faster that leads to complexity and also it requires higher storage space.

**Solution** –

- Mathematical computations are less
- Each authentication has their own procedure

**REFERENCE 9**

**TITLE** – Efficient Conditional Privacy-Preserving and Authentication Scheme for Secure Service Provision in VANET

**Concept** –

A conditional privacy-preserving and authentication scheme is proposed in this paper. This scheme is applicable to authenticate Vehicle-to-Vehicle communication and Vehicle-to-Infrastructure communication. For authenticating identity, pseudonym-based signatures are used. Vehicle verifies its real identity and tamper proof device password, then message is signed by tamper proof device and sent to RSU via OBU. In case of multiple requests arrives, it follows batch verification. First timestamp is noted, if timestamp is invalid the requests will be discarded.

**Problems** –

- If ID and password or leaked then a particular vehicle can be accessed by other malicious attackers.
• Complexity occurs in RSU due to verification of signature for all the requesting vehicle. RSU is also responsible to monitor other communications that is being held between vehicles present within its communication range.

Solution –

• RSU is responsible to authenticate head vehicles only

REFERENCE 10

TITLE – TAPCS-Traffic-aware pseudonym changing strategy for VANET

Concept –

This paper proposes location privacy in VANET using Traffic-Aware Pseudonym Changing Strategy. In this work, traffic congestion is detected and then an initiator is chosen after which the pseudonyms are changed. The initiator is responsible to create silent mix zone that consists of vehicles. Messages are broadcasted for message initiation and also for ending up the traffic congestion. Based on the changes in traffic density the pseudonym is generated for the vehicles for achieving security.

Problem –

Frequent changes in pseudonyms with respect to traffic on road lane, since the vehicles density varies often.

Solution –

Required security parameters are generated only for the requesting vehicles. The security related parameters unique and it is not necessary to be changed often.

REFERENCE 11

TITLE – Improved Dual Authentication and Key Management Techniques in Vehicular Ad Hoc Networks
Concept –

This paper involves with a dual authentication and key management technique for achieving security and quality of service. RSU registers to trusted authority, in which trusted authority involves with computation of two parameters. RSU is authenticated by these parameters and keys, then vehicles are authenticated using identity, hash code, nonces and others.

Problem –

- Authenticated by trusted authority increases burden in this entity.

Solution –

- Authentication responsibility is given to each entity only for authenticating a particular entity.

REFERENCE 12

**TITLE** – Distributed Aggregate Privacy-Preserving Authentication in VANETs

Concept –

In this paper the authors have proposed one-time identity based aggregate signature technique that is designed based on multiple trusted authorities. The procedure involves setup root trusted authority, setup lower level trusted authority, extract, sign and aggregate. In this work, RSU is considered to be lower level trusted authority, however this acts as one of the lower level trusted authority, the bogus message from a vehicle is predicted only by the root trusted authority. Finally the message authentication delay and loss rate are evaluated.
References


